This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－112751
（P2000－112751A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ 9/06	５５０Ｚ	５Ｂ０７６
				５５０Ｇ	５Ｂ０８５
	15/00	３３０	15/00	３３０Ｚ	

審査請求　未請求　請求項の数５　ＦＤ　（全 ８ 頁）

(21)出願番号　特願平10－300397

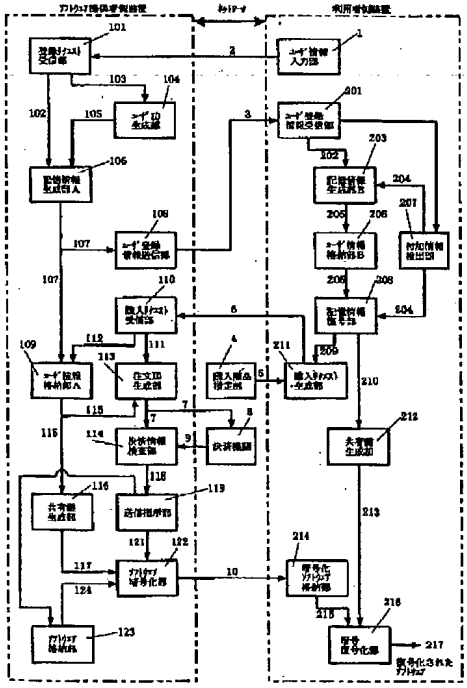
(22)出願日　平成10年10月７日(1998.10.7)

(71)出願人　000004167
日本コロムビア株式会社
東京都港区赤坂４丁目14番14号
(72)発明者　酒井　一重
東京都港区赤坂四丁目14番14号　日本コロムビア株式会社内
(74)代理人　100074550
弁理士　林　實

Ｆターム(参考)　5B076 FA06 FC10
5B085 AE02 AE13 AE29

(54)【発明の名称】　ソフトウエア流通システムに用いる装置

(57)【要約】
【課題】ソフトウエア流通システムにおいては、ソフトウエアの不正な複製及びその利用を防止することが困難であり、また、利用者の重要情報を保護することが困難であった。
【解決手段】ネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、利用者が入力した個人情報に基づいてユーザＩＤを生成する手段と、ユーザＩＤを記憶する手段と、ユーザＩＤに基づいて共有鍵を生成する手段と、生成した共有鍵で前記ソフトウエアを暗号化して伝送する手段と、共有鍵を用いて前記ソフトウエアを復号化する手段とを具備する。



1

【特許請求の範囲】

【請求項１】ネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、利用者が有する決済に関わる情報以外の個人情報に基づいて共有鍵を生成する手段と、生成した前記共有鍵により前記ソフトウエアを暗号化する手段とを具備することを特徴とするソフトウエア流通システムに用いる装置。

【請求項２】ネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、利用者が有する決済に関わる情報以外の個人情報に基づいて共有鍵を生成する手段と、暗号化された前記ソフトウエアを前記共有鍵を用いて復号化する手段とを具備することを特徴とするソフトウエア流通システムに用いる装置。

【請求項３】ソフトウエア提供者側装置と利用者側装置との間をネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、前記ソフトウエア提供者側装置は、前記利用者側装置から送信される個人情報を受信し前記個人情報と前記個人情報から生成したディジタルフィンガープリント情報とを複合した複合情報を生成する登録リクエスト受信部と、該登録リクエスト受信部が受信した前記個人情報に基づいてユーザＩＤを生成するユーザＩＤ生成部と、前記複合情報と前記ユーザＩＤとからユーザ情報を生成する記憶情報生成部と、前記ユーザ情報に変換処理を施して前記利用者側装置に送信するユーザ登録情報送信部と、前記ユーザ情報を格納するユーザ情報格納部と、前記利用者側装置からの指示により前記ユーザ情報に基づいて前記ソフトウエアを暗号化して出力する手段とを具備することを特徴とするソフトウエア流通システムに用いる装置。

【請求項４】請求項３記載のソフトウエア流通システムに用いる装置において、前記ソフトウエアを暗号化して出力する手段は、前記利用者側装置から出力された購入リクエストを受信したときユーザ情報格納部に登録されたユーザ情報を出力させる購入リクエスト受信部と、前記ユーザ情報格納部からの前記ユーザ情報を確認した後に前記購入リクエスト受信部からの発注情報を受け取り注文ＩＤを生成する注文ＩＤ生成部と、前記ユーザ情報格納部からの前記ユーザ情報に基づいて前記ソフトウエアを暗号化するために用いられる共有鍵を生成する共有鍵生成部と、複数の前記ソフトウエアを格納するソフトウエア格納部と、前記注文ＩＤ生成部で生成された前記注文ＩＤに基づいて前記ソフトウエア格納部に格納されている前記ソフトウエアを選択する送信指示部と、該送信指示部が選択した前記ソフトウエアを前記共有鍵を用いて暗号化する処理を行い出力するソフトウエア暗号化部とを具備したことを特徴とするソフトウエア流通システムに用いる装置。

2

【請求項５】ソフトウエア提供者側装置と利用者側装置との間をネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、前記利用者側装置は、ソフトウエア提供者側装置から送信されたユーザ登録情報を受信し前記ユーザ登録情報を暗号化されたユーザ情報へ変換するユーザ登録情報受信部と、前記ユーザ登録情報の前記ソフトウエア流通システムに依存した固有情報である付加情報を用いて前記暗号化されたユーザ情報を復号化する記憶情報復号部と、前記記憶情報復号部で復号化された前記ユーザ情報に基づいて共有鍵を生成する共有鍵生成部と、前記ソフトウエア提供者側装置から送信された暗号化ソフトウエアを格納する暗号化ソフトウエア格納部と、該暗号化ソフトウエア格納部に格納された前記暗号化ソフトウエアを前記共有鍵に基づいて復号化する暗号復号化部とを具備することを特徴とするソフトウエア流通システムに用いる装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ソフトウエアを流通・販売するソフトウエア流通システムに用いる装置に関する。

【０００２】

【従来の技術】計算機（例えば、パーソナル・コンピュータなど）及び計算機ネットワークの普及により、書籍、音楽、映画、テレビ番組などのディジタル化された著作物や、計算機プログラム、または、それらを使用するための使用許諾情報（パスワードや復号鍵を含む）などのソフトウエアや、コンピュータプログラムのようなコンピュータ上で機能するソフトウエアは、従来のような店舗販売を主体とする取引形態を用いなくても、電子商取引による決済とソフトウエアの流通が可能となった。

【０００３】このような電子商取引による決済とソフトウエアの流通が可能なソフトウエア流通システムにおいては、コンピュータでのデータ複製（コピー）など取り扱いが容易であり、一旦販売されたソフトウエアは容易に複製を作成することができるため、不正な複製を防止することが最大の課題であった。

【０００４】不正な複製を防止するために、最も広く使われるソフトウエアの保護手段としては、対象となるソフトウエアの使用に当たって必要なコード情報（鍵やパスワード情報など）の確認を行い、そのコード情報の入力があった場合のみ使用できる方法や、ソフトウエアそのものを何らかの方法で暗号化を施し、使用に当たっては鍵やパスワードを入力することで復号化する方法などが取られる。しかし、これらの方法を用いても、パスワードやデータを復号する鍵を複製することで、ソフトウエアの不正な複製が可能となるため、著作権利者にとって信頼できる保護手段であるとは言い難い。

【０００５】前記の問題点を解決する手法として、特開昭６４－６８８３５号公報によるソフトウエア権利管理制御方法がある。この方法では、暗号化されたソフトウエアを専用の復号化装置を用いて復号化しながら利用し、その装置において課金を行う。利用する度に課金をすることができ、暗号化されたソフトウエアは、複製することができても専用の復号化装置で復号化しないと利用できないため、不正な複製を無効なものとすることができる。一般に、この方法によるソフトウエア等の著作物の配布システムを超流通システムという。

【０００６】一方、電子商取引を行う際、決済に関わるクレジットカード情報や、それらとの対応づけが保証された準個人情報（パソコン通信サービスのユーザＩＤなど）をネットワークを通じて送信する場合には、それらの入力を要求する店舗側や決済代行機関と利用者側との間で、それらの情報を盗用して不正に利用しようとする第三者から情報を保護する手段が講じられる。

【０００７】とりわけ不特定な情報経路を通じて情報を交換するネットワーク（インタネットなど）を通じ、前記のような決済に関わる情報を送受信する際には、一般に鍵情報を保有する情報の送受信者以外の者が、暗号の復号化が困難と考えられる公開鍵暗号化方式が用いられることが多い。

【０００８】公開鍵暗号化方式を採用した暗号化通信技術によれば、利用者と信頼性をもつ店舗や決済処理機関との間でクレジットカード番号のように高い決済信用度を持つ情報を送受信することができる。しかし、購入対象が小額で、繰り返し、かつ、多数購入される性質のものであれば、購入毎にクレジットカード番号を入力するか、または、それらの代わりにクレジットカード番号、銀行口座番号の電子的格納部へのアクセスを行うための番号（ユーザＩＤとパスワードの組み合わせなど）を入力するなど手続が煩雑となり、極めて大きなアクセス障壁となる。

【０００９】また、クレジットカード番号のように社会的信用度の高い情報をネットワークを通じて送信する場合には、利用者側の電子商取引技術に対する信用度が利用のアクセス障壁となる場合もある。

【００１０】上記の問題を解決する手段として、特開平９－２４４８８６号公報に記載されているソフトウエア流通システムがある。このシステムでは、クレジットカード番号など決済に関わる重要情報や、それらとの対応づけが保証された識別情報（ユーザＩＤなど）や共有鍵を、店舗側のデータベースに記憶して、それらの情報を決済に使用している。利用者側では、会員登録時に記憶した識別情報を用いて購入の手続きを行うことにより、簡易な決済手続きを実現している。また、購入するソフトウエアは共有鍵で暗号化されており、ソフトウエアを使用するためには共有鍵が必要となるため、簡易なソフトウエアの複製を防止することができる。

【００１１】

【発明が解決しようとする課題】しかしながら、前述したような超流通システム等のソフトウエア流通システムにおいて、ソフトウエア提供者側がソフトウエアの不正な複製及びその利用を防止するためには、暗号化したソフトウエアを復号化する専用の復号化装置等のハードウエアを利用者に備えさせることが必要となる。

【００１２】そのため、利用者に専用の復号化装置等を配備させなければならないなど、初期費用が高くまた簡便性に欠けることから、ソフトウエア流通システムが産業的に普及しないという欠点がある。

【００１３】また、前述したような、利用者側が会員登録時に記憶した識別情報を用いて、簡易な決済手続きによりソフトウエアを購入することができるソフトウエア流通システムにおいては、ソフトウエア提供者側に、利用者のクレジットカード番号等の決済に関わる重要情報、識別情報および共有鍵をデータベースに記憶しておかなければならない。

【００１４】そのため、利用者が複数の店舗を利用する場合、複数の店舗毎にクレジットカード番号等の重要情報を登録しなければならないため、手続が面倒である。また、複数の店舗に利用者の重要情報を登録するため、利用者が自らの重要情報を保護することが困難であるという欠点がある。

【００１５】本発明は、ソフトウエアの不正な複製及びその利用を簡易な方法により防止すると共に、利用者の重要情報を保護することができるソフトウエア流通システムに用いる装置を提供することを目的としている。

【００１６】

【課題を解決するための手段】請求項１記載の本発明は、ネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、利用者が有する決済に関わる情報以外の個人情報に基づいて共有鍵を生成する手段と、生成した共有鍵によりソフトウエアを暗号化する手段とを具備することを特徴としている。

【００１７】請求項２記載の本発明は、ネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、利用者が有する決済に関わる情報以外の個人情報に基づいて共有鍵を生成する手段と、暗号化されたソフトウエアを共有鍵を用いて復号化する手段とを具備することを特徴としている。

【００１８】請求項３記載の本発明は、ソフトウエア提供者側装置と利用者側装置との間をネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、ソフトウエア提供者側装置は、利用者側装置から送信される個人情報を受信し、個人情報と個人情報から生成したディジタルフィンガープリント情報とを複合した複合情報を生成する登録リクエスト受信部と、登録リクエスト受信部が受信した個人情

報に基づいてユーザＩＤを生成するユーザＩＤ生成部と、複合情報とユーザＩＤとからユーザ情報を生成する記憶情報生成部と、ユーザ情報に変換処理を施して利用者側装置に送信するユーザ登録情報送信部と、ユーザ情報を格納するユーザ情報格納部と、利用者側装置からの指示によりユーザ情報に基づいてソフトウエアを暗号化して出力する手段とを具備することを特徴としている。

【００１９】請求項４記載の本発明は、請求項２記載のソフトウエア流通システムに用いる装置において、ソフトウエアを暗号化して出力する手段は、利用者側装置から出力された購入リクエストを受信したとき、ユーザ情報格納部に登録されたユーザ情報を出力させる購入リクエスト受信部と、ユーザ情報格納部からのユーザ情報を確認した後に、購入リクエスト受信部からの発注情報を受け取り注文ＩＤを生成する注文ＩＤ生成部と、ユーザ情報格納部からのユーザ情報に基づいてソフトウエアを暗号化するために用いられる共有鍵を生成する共有鍵生成部と、複数のソフトウエアを格納するソフトウエア格納部と、注文ＩＤ生成部で生成された注文ＩＤに基づいてソフトウエア格納部に格納されているソフトウエアを選択する送信指示部と、送信指示部が選択したソフトウエアを共有鍵を用いて暗号化する処理を行い出力するソフトウエア暗号化部とを具備したことを特徴としている。

【００２０】請求項５記載の本発明は、ソフトウエア提供者側装置と利用者側装置との間をネットワークを利用してソフトウエアを流通させるソフトウエア流通システムに用いる装置において、利用者側装置は、ソフトウエア提供者側装置から送信されたユーザ登録情報を受信し、当該ユーザ登録情報を暗号化されたユーザ情報へ変換するユーザ登録情報受信部と、ユーザ登録情報のソフトウエア流通システムに依存した固有情報である付加情報を用いて暗号化されたユーザ情報を復号化する記憶情報復号部と、記憶情報復号部で復号化されたユーザ情報に基づいて共有鍵を生成する共有鍵生成部と、ソフトウエア提供者側装置から送信された暗号化ソフトウエアを格納する暗号化ソフトウエア格納部と、暗号化ソフトウエア格納部に格納された暗号化ソフトウエアを共有鍵に基づいて復号化する暗号復号化部とを具備することを特徴としている。

【００２１】

【発明の実施の形態】図１は、本発明のソフトウエア流通システムに用いる装置における一実施例の概略構成を示す模式図である。図１において、ソフトウエア流通システムは、ソフトウエア提供者側装置と利用者側装置とを備え、これらの間での情報のやり取りは、ネットワークを介して行われる。

【００２２】利用者は、ソフトウエア流通システムの利用に当たって、先ず、利用者側装置のユーザ情報入力部１を用いて、利用者の氏名、所属、電子メールアドレス

などの個人情報２を入力し、ネットワークを通じて、ソフトウエア提供者側装置の登録リクエスト受信部１０１へ個人情報２を送信する。また、クレジットカードの番号や銀行口座の番号等の利用者の金銭に関する番号の情報は、決済に関わる情報として、前記個人情報には含まれない。

【００２３】ソフトウエア提供者側装置の登録リクエスト受信部１０１は、個人情報２のうちの、その利用者しか知り得ない情報（パスワード）や嗜好を表すプライバシー情報などの文字列からメッセージダイジェスト生成アルゴリズムによって変換生成される数値であるディジタルフィンガープリント情報を生成し、利用者との連絡に必須である個人情報２の部分情報（利用者名、電子メールアドレスなど）とディジタルフィンガープリント情報とを複合した複合情報１０２を生成する。

【００２４】また、ユーザＩＤ生成部１０４に対して未使用ユーザＩＤの割り当てを要求する割当要求情報１０３を発生して、ユーザＩＤ情報１０５の生成を促す。

【００２５】記憶情報生成部Ａ１０６は、複合情報１０２と割り当てられたユーザＩＤ情報１０５とから、ソフトウエア提供者側装置のデータベースであるユーザ情報格納部Ａ１０９に格納されるユーザ情報１０７を生成する。ユーザ情報１０７は、利用者を特定するために用いる情報である。

【００２６】ユーザ登録情報送信部１０８は、記憶情報生成部Ａ１０６からのユーザ情報１０７にネットワークにおける機密漏洩阻止を簡易に行うことを目的とした変換を施し、個人情報２を送信してきた利用者側装置のユーザ登録受信部２０１に、ユーザ登録情報３を返送する。

【００２７】利用者側装置のユーザ登録情報受信部２０１は、ユーザ登録情報送信部１０８と対称な変換により、ユーザ登録情報３からユーザ情報２０２への変換を実行する。ここで、個人情報２およびユーザ登録情報３のネットワーク間の送受信は、ＳＳＬ（Secure Socket Layer）プロトコルなどの公開鍵暗号化方式による通信を用いて行うことが好ましい。

【００２８】記録情報生成部Ｂ２０３は、ユーザ登録情報３の受信時に、付加情報検出部２０７によって検出されたソフトウエア流通システムに依存した固有情報である付加情報２０４を用いて暗号鍵を決定し、ユーザ登録情報受信部２０１から出力されたユーザ情報２０２を暗号化した暗号化ユーザ情報２０５をユーザ情報格納部Ｂ２０６に記憶させる。

【００２９】このように、ソフトウエア提供者側装置には、利用者の個人情報が蓄積されるが、クレジットカード情報などの重要な情報を含まないため、データベース管理者による悪用等の犯罪が発生する危険性が低く、利用者側から見た利用に対する不安感を軽減することができる。

【００３０】次に、ソフトウエア流通システムにおけるソフトウエアの購入からその利用までの処理動作を説明する。利用者側装置の購入リクエスト生成部２１１は、購入商品指定部４で指定された商品選択情報５を受領し、商品選択情報５に基づいて必要とする商品を選択し、ネットワークを通じてソフトウエア提供者側装置の購入リクエスト受信部１１０に購入リクエスト情報６を送信する。このことで、ソフトウエアの使用料の決済およびソフトウエア配送までの一連の動作が実行される。

【００３１】購入リクエスト情報６の送信に際して、記憶情報復号部２０８は、付加情報検出部２０７から、記憶情報生成部Ｂ２０３が暗号鍵を決定するために用いた付加情報２０４を取得して復号鍵を決定し、ユーザ情報格納部Ｂ２０６に記憶されている暗号化ユーザ情報２０５を復号化し、ユーザＩＤ情報２０９を購入リクエスト生成部２１１に通知する。

【００３２】購入リクエスト生成部２１１は、取得したユーザＩＤ情報２０９、商品選択情報（商品ＩＤ）５および購入リクエスト生成部２１１に予め設定された決済手段選択情報により、購入リクエスト情報６を生成して送信する。

【００３３】ここで、ＳＥＴ（Secure Electronic Transaction）またはＳＥＣＥ（SecureElectronic Commerce Environment）に準拠したクレジット決済方式電子財布を使用する場合には、購入リクエスト生成部２１１は、購入リクエスト６の送信に先行してソフトウエア提供者側装置のディジタル認証書、及び、利用者側装置のディジタル認証書を認証発行機関（図示せず）から取得し、ソフトウエア提供者側装置にクレジットカード番号、ディジタル認証書の送付を行う。

【００３４】ソフトウエア提供者側装置の購入リクエスト受信部１１０は、受信した購入リクエスト情報６から、商品選択情報（商品ＩＤ）５、ユーザＩＤ情報２０９および決済手段選択情報をデコードして、ユーザＩＤ選択情報１１２を生成する。

【００３５】そして、購入リクエスト受信部１１０は、ユーザＩＤ選択情報１１２を用いてユーザ情報格納部Ａ１０９に登録されたユーザ情報を指定する。ユーザ情報格納部Ａ１０９は、ユーザＩＤ選択情報１１２に基づいて注文ＩＤ生成部１１３にユーザ情報１１５を出力する。

【００３６】注文ＩＤ生成部１１３は、ユーザ情報格納部Ａ１０９からのユーザ情報１１５を確認後、購入リクエスト受信部１１０から商品ＩＤ、ユーザＩＤを含む発注情報１１１を受け取り、購入セッション毎に固有な番号である注文ＩＤを付加して、決済機関８への注文ＩＤ、商品ＩＤ、決済金額情報を含む決済承認要求７を送信する。

【００３７】決済情報検査部１１４は、決済承認要求７の応答として決済機関８から返送される決済承認通知９を受け取り、決済可否を判断し、決済が承認された場合に、送信指示部１１９に商品ＩＤを含む決済完了通知１１８を通知する。この決済機関８において、商品に対する金銭の支払いなどにおいては、利用者の決済に関わる情報が利用される。

【００３８】送信指示部１１９は、決済完了通知１１８で引き渡された商品ＩＤから、ソフトウエア格納部１２３に保管されている該ソフトウエアを選択し、ソフトウエア暗号化部１２２に出力する指示を行う。ソフトウエア格納部１２３は、送信指示部１１９の指示に基づいて、選択されたソフトウエア１２４をソフトウエア暗号化部１２２に出力する。

【００３９】また、送信指示部１１９は、ソフトウエア暗号化部１２２から出力されたソフトウエアの暗号化の実行とネットワーク配送を指示をする送信指示１２１を、ソフトウエア暗号化部１２２に通知する。

【００４０】ソフトウエア暗号化部１２２におけるソフトウエアへの暗号化の実行に先行して、ユーザ情報格納部Ａ１０９のユーザ情報１１５は、共有鍵生成部１１６によりソフトウエアを暗号化するのに用いられる共有鍵１１７に変換され、ソフトウエア暗号化部１２２に送られる。

【００４１】この共有鍵は、利用者が購入したソフトウエアを復号化することにのみ使用され、他の目的には利用できないため、盗難を試みうようとする犯罪の発生率は低く、簡易なシステムにより、ソフトウエアの不正な複製及びその利用を防止することができる。

【００４２】また、共有鍵の生成に関して情報源となる個人情報を格納する際に、利用者側装置の環境情報（ＣＰＵ（Central Processor Unit）の識別番号、ディスクボリューム識別など）を抽出する付加情報検出手段と、付加情報検出手段によって検出された情報を用いて暗号化を実行する手段とを用いて暗号化したユーザ情報を格納することによって、共有鍵の生成アルゴリズム解析への糸口を隠蔽し、共有鍵の盗難をより困難なものとすることができる。

【００４３】ソフトウエア暗号化部１２２は、送信指示部１１９の指示に基づいて、共有鍵生成部１１６からの共有鍵１１７を用いてソフトウエア格納部１２３からのソフトウエア１２４を暗号化する。

【００４４】ソフトウエア暗号化部１２２で暗号化された暗号化ソフトウエア１０は、ネットワークを介して利用者側装置の暗号化ソフトウエア格納部２１４へとダウンロードされ保存され、購入に関わるセッションの一切が終了する。

【００４５】購入したソフトウエアを使用する場合、暗号化ソフトウエア格納部２１４に保存された暗号化ソフトウエア１０は、暗号復号化部２１６において共有鍵生成部２１２で生成される暗号復号鍵２１３を用いて復号化される。

【００４６】利用者側装置の共有鍵生成部２１２は、ソフトウエア提供者側装置の共有鍵生成部１１６と同一手順により、暗号復号鍵２１３が生成される。暗号復号鍵２１３を生成する際、記憶情報復号部２０８は、付加情報検出部２０７によって検出された付加情報２０４を用いて、ユーザ情報格納部Ｂ２０６に暗号化され格納されたユーザ情報２０５を復号化する。ここで、ソフトウエアは、実行時に、その都度復号化され、復号化されたソフトウエアを稼動するハードウェア内に残さないことが望ましい。

【００４７】このように、ソフトウエア流通システムにおいて、決済に関わらないユーザ情報をソフトウエア提供者側装置と利用者側装置とで共有し、その情報に基づいて共有鍵を決定して生成し、生成した共有鍵で該ソフトウエアを暗号化してソフトウエア提供者側装置から利用者側装置に配送する。利用者側装置においては、同様の共有鍵を生成する手段を用いて生成される共有鍵により配送された該ソフトウエアを復号化する。

【００４８】したがって、ソフトウエア提供者側装置から利用者側装置に対して暗号化されたソフトウエアを送信する際に使用する共有鍵は、ソフトウエア流通システムの機能動作時に生成されるため、共有鍵が盗難される可能性を極めて低くすることができる。

【００４９】以上のように、本実施例によれば、ソフトウエア提供者側装置に登録したユーザ情報に基づいて、利用者側装置は、固有の共有鍵で暗号化されたソフトウエアを受領するため、同じ共有鍵を発生しうるユーザ情報を保有する利用者側装置でなければ利用できないソフトウエア流通システムを実現することができる。

【００５０】また、本実施例で示す利用者側装置を、全てパーソナル・コンピュータで実行することができる応用ソフトウエアとして実現すれば、安価で利用しやすいソフトウエア流通システムが実現する。

【００５１】また、付加情報が利用者側装置の稼動するハードウェア環境の固有パラメータ（ＣＰＵの識別番号、ディスクボリューム番号など）を付加情報２０４として抽出することで、ユーザ情報格納部Ｂ２０６に暗号化され保存されたユーザ情報は、他のハードウェア環境では復号化することができないため、利用者側装置において、ソフトウエアを不正に複製して利用することを防止することができる。

【００５２】また、ソフトウエア提供者側装置において、各ソフトウエアの購入数、利用者、日時を正確に記録する手段を用いることにより、小額ソフトウエアに関する著作権使用料などの計算を実施することができる。各ソフトウエアの利用者を記録することで顧客サービスの拡張も容易に実施できる。

【００５３】決済に関してソフトウエア提供者側装置は、利用者の選択した決済手段が規定する決済プロトコルで通信する手段と、外部決済手段の承認を確認する手段を用いて、ソフトウエア利用課金集計のみを行う。各種決済手段との通信には、例えば、クレジットカードを用いた決済の場合には、ＳＥＴ仕様や、ＳＥＣＥ仕様に準じた電子決済プログラムを利用者側で別途使用することで安全かつ簡便な決済を利用することができる。

【００５４】また、本実施例のソフトウエア提供者側装置において、ユーザに関する情報を格納し、ユーザＩＤ等からユーザを確認するユーザ認証部と、利用者側装置からの購入リクエストを受信し、決済した後、ソフトウエアの送信を実行するソフトウエア送信部とを、別々の装置としてもよい。つまり、ユーザ認証部は、登録リクエスト受信部１０１と、ユーザＩＤ生成部１０４、記憶情報生成部Ａ１０６、ユーザ登録情報送信部１０８及びユーザ情報格納部Ａ１０９を備え、ソフトウエア送信部は、購入リクエスト受信部１１０、注文ＩＤ生成部１１３、決済情報検査部１１４、共有鍵生成部１１６、送信指示部１１９、ソフトウエア暗号化部１２２及びソフトウエア格納部１２３を備えた構成にしてもよい。

【００５５】ユーザ情報格納部を備えるユーザ認証部とソフトウエア送信部との間で送受信される通信内容（ユーザＩＤ選択１１２、及び、ユーザ情報１１５）を、ＳＳＬなどの公開暗号鍵方式の暗号化通信により保護することで、前述した実施例と同じ機能を、複数のソフトウエア送信部で実施することができる。

【００５６】

【発明の効果】本発明によれば、ソフトウエア提供者装置に送信する情報が、利用者のクレジットカード番号などの決済手段として大きな効力を持つ情報を登録する必要がなく、簡易に幅広い利用者が流通システムを利用することが可能であり、かつ、利用者側の心因的アクセス障壁を小さなものとすることが可能である。

【００５７】また、提供されるソフトウエアは、利用者毎に異なる共有鍵で暗号化されて配送されるため、ソフトウエアを不正に複製し利用することを防止することができる。

【００５８】更に、悪意をもって共有鍵を盗用し、取得したソフトウエアを再流通しようとする者に対しても、共有鍵そのものが利用者側装置に永続的に存在しないため、盗用を極めて困難なものとすることができる。

【図面の簡単な説明】

【図１】本発明のソフトウエア流通システムに用いる装置における一実施例の概略構成を示す模式図。

【符号の説明】

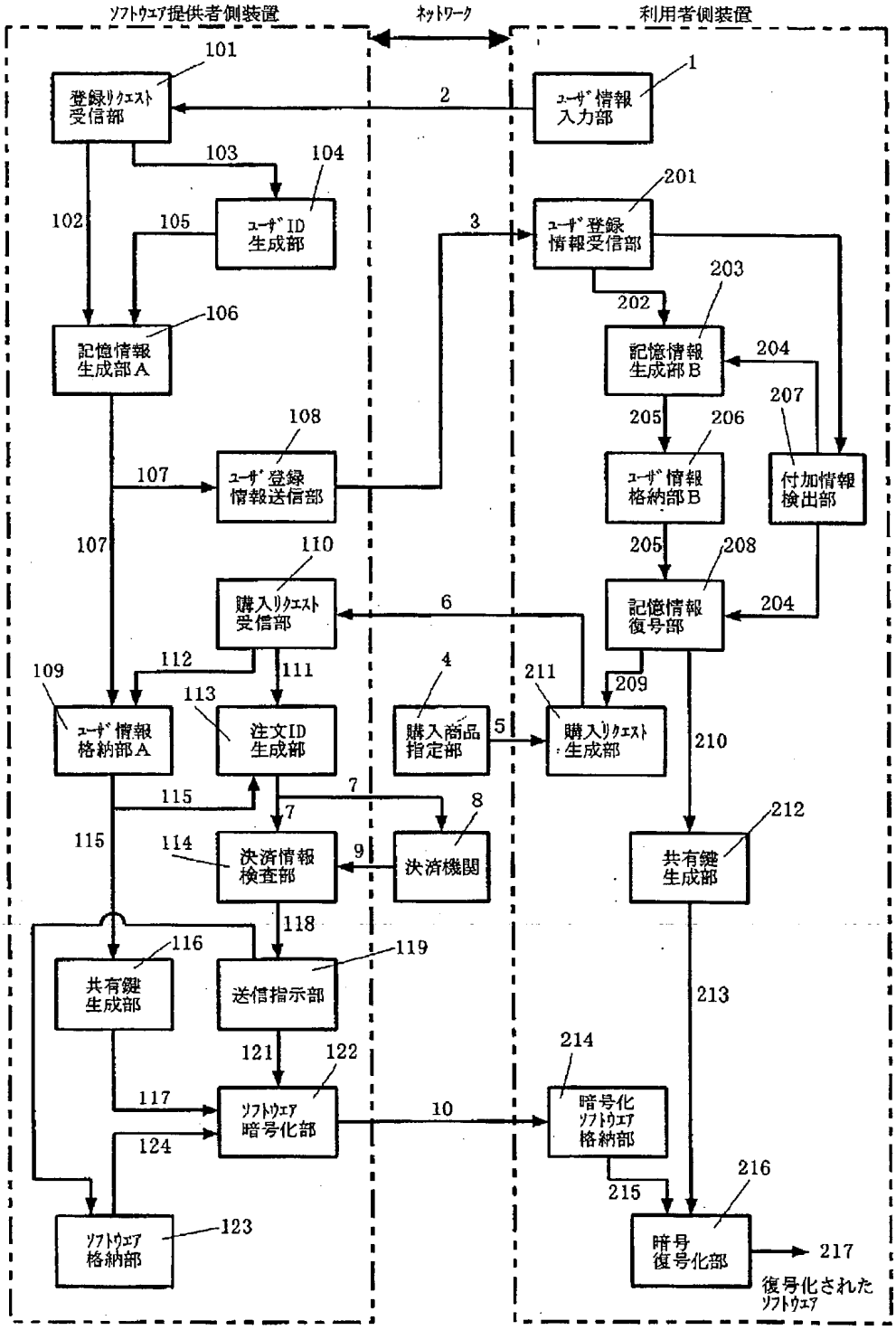
１・・ユーザ情報入力部、４・・購入商品指定部、８・・決済機関、１０１・・登録リクエスト受信部、１０４・・ユーザＩＤ生成部、１０６・・記憶情報生成部Ａ、１０８・・ユーザ登録情報送信部、１０９・・ユーザ情報格納部Ａ、１１０・・購入リクエスト受信部、１１３・・注文ＩＤ生成部、１１４・・決済情報検査部、１１６・・共有鍵生成部、１１９・・送信指示部、１２２・

11

・ソフトウエア暗号化部、１２３・・ソフトウエア格納部、２０１・・ユーザ登録情報受信部、２０３・・記憶情報生成部Ｂ、２０６・・ユーザ情報格納部Ｂ、２０７・・付加情報検出部、２０８・・記憶情報復号部、２１１・・購入リクエスト生成部、２１２・・共有鍵生成部、２１４・・暗号化ソフトウエア格納部、２１６・・暗号復号化部。

12

【図１】


ソフトウエア提供者側装置
ネットワーク
利用者側装置
登録リクエスト受信部
ユーザ情報入力部
ユーザID生成部
ユーザ登録情報受信部
記憶情報生成部A
記憶情報生成部B
ユーザ登録情報送信部
ユーザ情報格納部B
付加情報検出部
購入リクエスト受信部
記憶情報復号部
ユーザ情報格納部A
注文ID生成部
購入商品指定部
購入リクエスト生成部
決済情報検査部
決済機関
共有鍵生成部
共有鍵生成部
送信指示部
ソフトウエア暗号化部
暗号化ソフトウエア格納部
ソフトウエア格納部
暗号復号化部
復号化されたソフトウエア

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-112751
(43)Date of publication of application : 21.04.2000

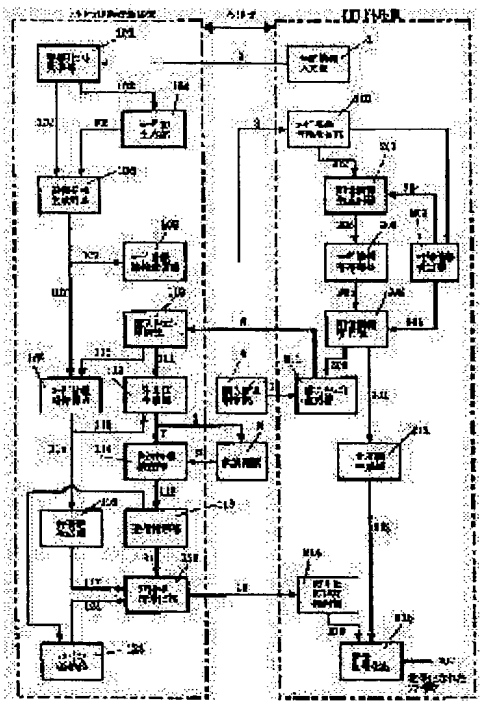
(51)Int.CI. G06F 9/06
G06F 15/00

(21)Application number : 10-300397
(22)Date of filing : 07.10.1998

(71)Applicant : NIPPON COLUMBIA CO LTD
(72)Inventor : SAKAI KAZUSHIGE

(54) DEVICE USED FOR SOFTWARE DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent illegal copy and its use and also to protect user's important information by enciphering software by a shared key generated, based on specific personal information.
SOLUTION: A transmission instructing part 119 selects software 124 stored in a software storing part 123 from a product ID delivered by a settlement completion notice 118 and outputs it to a software enciphering part 122. The user information 115 of a user information storing part A 109 converts the software into a shared key 117 to be used for encipher by a shared key generating part 116 and sends it to the part 122 before executing the encipher of the software. The part 119 notifies a transmission instruction 121 which instructs the execution of software encipher and network delivery to the part 122. The shared key is used only to decode software purchased by a user and prevents illegal copy of the software and its use.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

[JP,2000-112751,A]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

[Claim(s)]

[Claim 1] Equipment used for the software negotiation system characterized by to provide a means generate a share key based on individual humanity news other than the information in connection with the settlement of accounts which a user has in the equipment used for the software negotiation system which circulates software using a network, and a means encipher said software with said generated share key.

[Claim 2] Equipment used for the software negotiation system characterized by to provide a means generate a share key based on individual humanity news other than the information in connection with the settlement of accounts which a user has in the equipment used for the software negotiation system which circulates software using a network, and a means decrypt said enciphered software using said share key.

[Claim 3] In the equipment which uses between software provider side equipment and user side equipment for the software negotiation system which circulates software using a network With the registration request receive section which generates the compound information which compounded the digital fingerprints information which said software provider side equipment received the individual humanity news transmitted from said user side equipment, and was generated from said individual humanity news and said individual humanity news The user ID generation section which generates user ID based on said individual humanity news which this registration request receive section received, The storage information generation section which generates User Information from said compound information and said user ID, The user registration information transmitting section which performs transform processing to said User Information, and transmits to said user side equipment, Equipment used for the software negotiation system characterized by providing the User Information storing section which stores said User Information, and a means to encipher said software based on said User Information with the directions from said user side equipment, and to output.

[Claim 4] A means to encipher and output said software in the equipment used for a software negotiation system according to claim 3 With the purchase request receive section which makes User Information registered into the User Information storing section when the purchase request outputted from said user side equipment was received output Order ID generation section which generates the reception order ID for the ordering information from said purchase request receive section after checking said User Information from said User Information storing section, The share key generation section which generates the share key used in order to encipher said software based on said User Information from said User Information storing section, The software storing section which stores said two or more software, and the transmitting directions section which chooses said software stored in said software storing section based on said order ID generated in said order ID generation section, Equipment used for the software negotiation system characterized by providing the software encryption section which outputs by performing processing which enciphers said software which this transmitting directions section chose using said share key.
[Claim 5] In the equipment which uses between software provider side equipment and user side equipment for the software negotiation system which circulates software using a network said user side equipment With the user registration information receive section which changes into User Information which the user registration information transmitted from software provider side equipment was received [User Information], and had said user registration information enciphered The storage information decode section which decrypts said enciphered User Information using the additional information which is the proper information depending on said software negotiation system of said user registration information, The share key generation section which generates a share key based on said User Information decrypted in said storage information decode section, The encryption software storing section which stores the encryption software transmitted from said software provider side equipment, Equipment used for the software negotiation system characterized by providing the code decryption section which decrypts said encryption software stored in this encryption software storing section based on said share key.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the equipment which uses software for the software negotiation system circulated and sold.
[0002]

[Description of the Prior Art] Even if the dealings gestalt which makes a store sale like before a subject was not used for software, such as a work digitized [TV program / books, music, the film,] by the spread of computers (for example, personal computer etc.) and computer networks, and activity consent information (a password and a decode key are included) for using a computer program or them, and the software which functions on a computer like a computer program, the negotiation of the settlement of accounts by electronic commerce and software of it was attained.

[0003] In the software negotiation system which can circulate the settlement of accounts by such electronic commerce, and software, handling, such as a data duplicate (copy) in a computer, was easy, and since the once sold software created a duplicate easily, it was the biggest technical problem to prevent an unjust duplicate.

[0004] The approach of using it, only when required code information is checked in the activity of the target software as a safeguard of the software most widely used in order to prevent an unjust duplicate (a key, password information, etc.) and there is an input of the code information, the approach of decrypting in enciphering the software itself by a certain approach, and entering a key and a password in an activity, etc. are taken. However, since the unjust duplicate of software is attained with reproducing the key which decodes a password and data even if it uses these approaches, it is hard to say that it is a safeguard reliable for a writing rightful claimant.

[0005] As the technique of solving the aforementioned trouble, there is the software access supervisory control approach by JP,64-68835,A. By this approach, it uses decrypting the enciphered software using the decryption equipment of dedication, and charges in that equipment. Since it cannot be used unless it decrypts it with the decryption equipment of dedication, even if it can reproduce the software which could charge whenever it used, and was enciphered, it can make unjust reproduction invalid. Generally, the distribution system of works, such as software by this approach, is called superdistribution system.

[0006] On the other hand, in case electronic commerce is performed, when transmitting the credit card information in connection with settlement of accounts, and the semi- individual humanity news (user ID of personal computer communication service etc.) to which matching with them was guaranteed through a network, a means to protect information from the third party who is going to plagiarize those information and is going to use unjustly between the store which requires those inputs and settlement-of-accounts agencies and user sides is provided.

[0007] In case the information in connection with the above settlement of accounts is transmitted and received through the networks (Internet etc.) which exchange

information through an especially unspecified information path, the public-key-encryption-ized method with which persons other than the transceiver person of the information which generally holds key information are considered that a decryption of a code is difficult is used in many cases.

[0008] According to the encryption communication technology which adopted the public-key-encryption-ized method, the information which has high settlement-of-accounts credibility like a credit card number among the stores and settlement-of-accounts processing engines which have dependability with a user can be transmitted and received. However, if the object for purchase is the thing of the property by which a large number purchase is carried out at a small sum, it will input a credit card number for every purchase, or it will become complicated taking the necessary procedure it, such as to input the numbers (combination of user ID and a password etc.) for performing access to the electronic storing section of a credit card number and the bank account number to instead of [those], and it serves as a very big access obstruction.

[0009] Moreover, when transmitting the information that social credibility is high, through a network like a credit card number, the credibility over the electronic commerce technique by the side of a user may serve as an access obstruction of utilization.

[0010] As a means to solve the above-mentioned problem, there is a software negotiation system indicated by JP,9-244886,A. In this system, a credit card number etc. memorizes the critical information in connection with settlement of accounts, the identification information (user ID etc.) to which matching with them was guaranteed, and a share key in the database by the side of a store, and those information is used for settlement of accounts. In the user side, simple settlement-of-accounts procedure is realized by taking the necessary procedure for purchase using the identification information memorized at the time of member registration. Moreover, it is enciphered with the share key, and since a share key is needed in order to use software, the software to purchase can prevent the duplicate of simple software.

[0011]

[Problem(s) to be Solved by the Invention] However, in software negotiation systems, such as a superdistribution system which was mentioned above, in order for a software provider side to prevent the unjust duplicate of software, and its utilization, it is necessary to make a user have hardware, such as decryption equipment of the dedication which decrypts the enciphered software.

[0012] Therefore, since front-end cost lacks in simple nature highly again, there is a

fault that a software negotiation system does not spread industrially — a user must be made to arrange the decryption equipment of dedication etc..

[0013] Moreover, a user side who mentioned above must memorize a user's critical information, identification information, and share key in connection with settlement of a credit card number etc. in a database at a software provider side in the software negotiation system which can purchase software in a simple settlement-of-accounts procedure using the identification information memorized at the time of member registration.

[0014] Therefore, a procedure is troublesome in order to have to register critical information, such as a credit card number, for two or more stores of every, when a user uses two or more stores. Moreover, in order to register a user's critical information into two or more stores, there is a fault that it is difficult for a user to protect his critical information.

[0015] This invention aims at offering the equipment used for the software negotiation system which can protect a user's critical information while it prevents the unjust duplicate and its utilization of software by the simple approach.

[0016]

[Means for Solving the Problem] This invention according to claim 1 is characterized by providing a means to generate a share key based on individual humanity news other than the information in connection with the settlement of accounts which a user has, and a means to encipher software with the generated share key in the equipment used for the software negotiation system which circulates software using a network.

[0017] This invention according to claim 2 is characterized by providing a means to generate a share key based on individual humanity news other than the information in connection with the settlement of accounts which a user has, and a means to decrypt the enciphered software using a share key in the equipment used for the software negotiation system which circulates software using a network.

[0018] In the equipment with which this invention according to claim 3 uses between software provider side equipment and user side equipment for the software negotiation system which circulates software using a network With the registration request receive section which generates the compound information which software provider side equipment received the individual humanity news transmitted from user side equipment, and compounded individual humanity news and the digital fingerprints information generated from individual humanity news The user ID generation section which generates user ID based on the individual humanity news which the registration request receive section received, The storage information generation section which

generates User Information from compound information and user ID, It is characterized by providing the user registration information transmitting section which performs transform processing to User Information and transmits to user side equipment, the User Information storing section which stores User Information, and a means to encipher software based on User Information with the directions from user side equipment, and to output.

[0019] A means for this invention according to claim 4 to encipher software in the equipment used for a software negotiation system according to claim 2, and to output With the purchase request receive section which makes User Information registered into the User Information storing section output when the purchase request outputted from user side equipment is received Order ID generation section which generates the reception order ID for the ordering information from a purchase request receive section after checking User Information from the User Information storing section, The share key generation section which generates the share key used in order to encipher software based on User Information from the User Information storing section, The software storing section which stores two or more software, and the transmitting directions section which chooses the software stored in the software storing section based on the order ID generated in order ID generation section, It is characterized by providing the software encryption section which outputs by performing processing which enciphers the software which the transmitting directions section chose using a share key.

[0020] In the equipment with which this invention according to claim 5 uses between software provider side equipment and user side equipment for the software negotiation system which circulates software using a network With the user registration information receive section which changes into User Information which user side equipment received [User Information] the user registration information transmitted from software provider side equipment, and had the user registration information concerned enciphered The storage information decode section which decrypts User Information enciphered using the additional information which is the proper information depending on the software negotiation system of user registration information, The share key generation section which generates a share key based on User Information decrypted in the storage information decode section, It is characterized by providing the encryption software storing section which stores the encryption software transmitted from software provider side equipment, and the code decryption section which decrypts the encryption software stored in the encryption software storing section based on a share key.

[0021]

[Embodiment of the Invention] Drawing 1 is the mimetic diagram showing the outline configuration of one example in the equipment used for the software negotiation system of this invention. In drawing 1 , a software negotiation system is equipped with software provider side equipment and user side equipment, and the exchange of the information between these is performed through a network.

[0022] In utilization of a software negotiation system, first, using the User Information input section 1 of user side equipment, a user inputs the individual humanity news 2, such as a user's name, affiliation, and an e-mail address, and transmits the individual humanity news 2 to the registration request receive section 101 of software provider side equipment through a network. Moreover, the information on the number about the money of users, such as a number of a credit card and a number of a bank account, is not included in said individual humanity news as information in connection with settlement of accounts.

[0023] The registration request receive section 101 of software provider side equipment generates the digital fingerprints information which is the numeric value by which conversion generation is carried out with a message digest generation algorithm from character strings, such as the privacy information showing the information (password) which only the user of the individual humanity news 2 cannot know, or taste, and generates the compound information 102 which compounded the partial information (the user name, e-mail address, etc.) and the digital fingerprints information on the indispensable individual humanity news 2 with communication with a user.

[0024] Moreover, the allocation demand information 103 that assignment of intact user ID is required from the user ID generation section 104 is generated, and generation of the user ID information 105 is urged.

[0025] The storage information generation section A106 generates User Information 107 stored in the User Information storing section A109 which is the database of software provider side equipment from the compound information 102 and the assigned user ID information 105. User Information 107 is information used since a user is specified.

[0026] The user registration information transmitting section 108 performs conversion aiming at carrying out leakage-of-secrets inhibition in a network to User Information 107 simply from the storage information generation section A106, and returns the user registration information 3 to the user registration receive section 201 of user side equipment which has transmitted the individual humanity news 2.

[0027] The user registration information receive section 201 of user side equipment performs conversion to User Information 202 from the user registration information 3 by symmetrical conversion with the user registration information transmitting section 108. It is desirable to perform the transmission and reception between the networks of the individual humanity news 2 and the user registration information 3 here using the communication link by public-key-encryption-ized methods, such as a SSL (Secure Socket Layer) protocol.

[0028] The recording information generation section B203 determines a cryptographic key using the additional information 204 which is the proper information depending on the software negotiation system detected by the additional information detecting element 207 at the time of reception of the user registration information 3, and makes the User Information storing section B206 memorize encryption User Information 205 which enciphered User Information 202 outputted from the user registration information receive section 201.

[0029] Thus, although a user's individual humanity news is accumulated in software provider side equipment, since information with important credit card information etc. is not included, the danger that crimes, such as improper use by the database manager, will occur is low, and can mitigate the insecurity over the utilization seen from the user side.

[0030] Next, the processing actuation from the purchase of the software in a software negotiation system to the utilization is explained. The purchase request generation section 211 of user side equipment receives the goods selection information 5 specified with the purchase goods specification part 4, chooses the goods needed based on the goods selection information 5, and transmits the purchase request information 6 to the purchase request receive section 110 of software provider side equipment through a network. By this, a series of actuation to settlement of accounts and software delivery of the dues of software is performed.

[0031] On the occasion of transmission of the purchase request information 6, the storage information decode section 208 acquires the additional information 204 used in order that the storage information generation section B203 might determine a cryptographic key from the additional information detecting element 207, determines a decode key, decrypts encryption User Information 205 memorized by the User Information storing section B206, and notifies the user ID information 209 to the purchase request generation section 211.

[0032] By the payment system selection information beforehand set as the user ID information 209, the goods selection information (goods ID) 5, and the purchase

request generation section 211 which were acquired, the purchase request generation section 211 generates the purchase request information 6, and transmits.

[0033] Here, in using the credit settlement method smart card based on SET (Secure Electronic Transaction) or SECE (SecureElectronic Commerce Environment), the purchase request generation section 211 is preceded with transmission of the purchase request 6, acquires the digital certificate of attestation of software provider side equipment, and the digital certificate of attestation of user side equipment from an authentication issuance engine (not shown), and performs sending of a credit card number and a digital certificate of attestation to software provider side equipment.

[0034] From the received purchase request information 6, the purchase request receive section 110 of software provider side equipment decodes the goods selection information (goods ID) 5, the user ID information 209, and payment system selection information, and generates the user ID selection information 112.

[0035] And the purchase request receive section 110 specifies User Information registered into the User Information storing section A109 using the user ID selection information 112. The User Information storing section A109 outputs User Information 115 to order ID generation section 113 based on the user ID selection information 112.

[0036] Order ID generation section 113 adds the order ID which is a peculiar number for every reception and purchase session about the ordering information 111 which contains Goods ID and user ID from the purchase request receive section 110 after checking User Information 115 from the User Information storing section A109, and transmits the settlement-of-accounts need for approval 7 including Order ID, Goods ID, and settlement-of-accounts amount-of-money information to the settlement-of-accounts engine 8.

[0037] The settlement-of-accounts information Banking Inspection Department 114 notifies the advice 118 of the completion of settlement of accounts which contains Goods ID in the transmitting directions section 119, when reception and settlement-of-accounts propriety are judged and settlement of accounts is recognized in the advice 9 of settlement-of-accounts acknowledgement returned by the settlement-of-accounts engine 8 as a response of the settlement-of-accounts need for approval 7. In this settlement-of-accounts engine 8, the information in connection with settlement of accounts of a user is used in the payment of money to goods etc.

[0038] The transmitting directions section 119 chooses this software currently kept by the software storing section 123 from the goods ID handed over by the advice 118 of the completion of settlement of accounts, and performs the directions outputted to

the software encryption section 122. The software storing section 123 outputs the selected software 124 to the software encryption section 122 based on directions of the transmitting directions section 119.

[0039] Moreover, the transmitting directions section 119 notifies the transmitting directions 121 which direct activation and network delivery of encryption of the software outputted from the software encryption section 122 to the software encryption section 122.

[0040] It precedes with activation of the encryption to the software in the software encryption section 122, and User Information 115 of the User Information storing section A109 is changed into the share key 117 used for enciphering software by the share key generation section 116, and is sent to the software encryption section 122.

[0041] since this share key is used only for decrypting the software which the user purchased and cannot be used for other objects, the incidence rate of the crime which can try a theft is low, and can prevent the unjust duplicate and its utilization of software by the simple system.

[0042] Moreover, in case the individual humanity news which serves as the information source about generation of a share key is stored An additional information detection means to extract the environmental information (the identification number of CPU (Central Processor Unit), disk volume discernment, etc.) of user side equipment, By storing User Information enciphered using a means to perform encryption using the information detected by the additional information detection means, the clue to the generation algorithm analysis of a share key can be concealed, and the theft of a share key can be made more difficult.

[0043] The software encryption section 122 enciphers the software 124 from the software storing section 123 using the share key 117 from the share key generation section 116 based on directions of the transmitting directions section 119.

[0044] Through a network, the encryption software 10 enciphered in the software encryption section 122 is downloaded to the encryption software storing section 214 of user side equipment, and is saved, and all of the session in connection with purchase ends it.

[0045] When using the purchased software, the encryption software 10 saved in the encryption software storing section 214 is decrypted using the code decode key 213 generated in the share key generation section 212 in the code decryption section 216.

[0046] As for the share key generation section 212 of user side equipment, the code decode key 213 is generated by the same procedure as the share key generation section 116 of software provider side equipment. In case the code decode key 213 is

generated, the storage information decode section 208 decrypts User Information 205 which was enciphered by the User Information storing section B206, and was stored in it using the additional information 204 detected by the additional information detecting element 207. Here, as for software, it is desirable for it to be decrypted each time at the time of activation, and not to leave the decrypted software in the hardware which works.

[0047] Thus, in a software negotiation system, software provider side equipment and user side equipment share User Information without regards to settlement of accounts, this software is enciphered with the share key which determined, generated and generated the share key based on the information, and it delivers from software provider side equipment to user side equipment. In user side equipment, this software delivered with the share key generated using a means to generate the same share key is decrypted.

[0048] Therefore, since the share key used in case the software enciphered from software provider side equipment to user side equipment is transmitted is generated at the time of functional actuation of a software negotiation system, it can make very low possibility that the theft of the share key will be carried out.

[0049] As mentioned above, since the software as which user side equipment was enciphered with the share key of a proper based on User Information registered into software provider side equipment according to this example is received, the software negotiation system which cannot be used if it is not user side equipment which holds User Information which may generate the same share key is realizable.

[0050] Moreover, the software negotiation system which will be cheap and will be easy to use all the user side equipments shown by this example if it realizes as application software which can be performed with a personal computer is realized.

[0051] Moreover, in other hardware environments, since User Information from which additional information was enciphered and saved in the User Information storing section B206 by extracting the proper parameters (the identification number of CPU, disk volume number, etc.) of the hardware environment where user side equipment works, as additional information 204 cannot be decrypted, it can prevent reproducing software unjustly and using it in user side equipment.

[0052] Moreover, in software provider side equipment, the royalty about small sum software etc. is calculable by using a means to record the number of purchase of each software, a user, and time on accuracy. The escape of customer service can also be easily carried out by recording the user of each software.

[0053] Software provider side equipment performs only a software utilization

accounting total using a means to communicate with the settlement-of-accounts protocol which the payment system which the user chose specifies, and a means to check acknowledgement of an external payment system, about settlement of accounts. In the settlement of accounts which used the credit card for the communication link with various payment systems, insurance and simple settlement of accounts can be used by using separately the electronic banking program according to a SET specification and a SECE specification by the user side.

[0054] Moreover, in the software provider side equipment of this example, the information about a user is stored and the user authentication section which checks a user from user ID etc., and the purchase request from user side equipment are received, and after settling accounts, it is good also considering the software transmitting section which performs transmission of software as separate equipment. That is, the user-authentication section may have the registration request receive section 101, the user ID generation section 104 and the storage information generation section A106, the user-registration information transmitting section 108, and the User Information storing section A109, and the software transmitting section may carry out to the configuration which it had in the purchase request receive section 110, order ID generation section 113, the settlement-of-accounts information Banking Inspection Department 114, the share key generation section 116, the transmitting directions section 119, the software encryption section 122, and the software storing section 123.

[0055] The same function as the example which mentioned above the content of a communication link (the user ID selection 112 and User Information 115) transmitted and received between the user authentication sections and the software transmitting sections equipped with the User Information storing section by protecting by the encryption communication link of open cryptographic key methods, such as SSL, can be carried out in two or more software transmitting sections.

[0056]

[Effect of the Invention] According to this invention, a simply broad user is able not to register the information in which the information transmitted to software provider equipment has the big validity as payment systems, such as a user's credit card number, and to use a negotiation system, and it is possible to make the psychogenesis-access obstruction by the side of a user into a small thing.

[0057] Moreover, since the software offered is enciphered and delivered with a different share key for every user, it can prevent reproducing software unjustly and using it.

[0058] Furthermore, since the share key itself does not exist permanently the software which used by stealth and acquired the share key with malice in user side equipment to those who are going to re-circulate, surreptitious use can be made very difficult.

[Brief Description of the Drawings]

[Drawing 1] The mimetic diagram showing the outline configuration of one example in the equipment used for the software negotiation system of this invention.

[Description of Notations]

1 .. The User Information input section, 4 .. A purchase goods specification part, 8 .. Settlement-of-accounts engine, 101 .. A registration request receive section, 104 .. The user ID generation section, 106 .. Storage information generation section A 108 .. The user registration information transmitting section, 109 .. User Information storing section A 110 .. A purchase request receive section, 113 .. Order ID generation section, 114 .. Settlement-of-accounts information Banking Inspection Department, 116 .. The share key generation section, 119 .. The transmitting directions section, 122 .. Software encryption section, 123 .. The software storing section, 201 .. User registration information receive section, 203 [.. The storage information decode section, 211 / .. The purchase request generation section, 212 / .. The share key generation section, 214 / .. The encryption software storing section, 216 / .. Code decryption section.] .. The storage information generation section B, 206 .. The User Information storing section B, 207 .. An additional information detecting element, 208

[Translation done.]

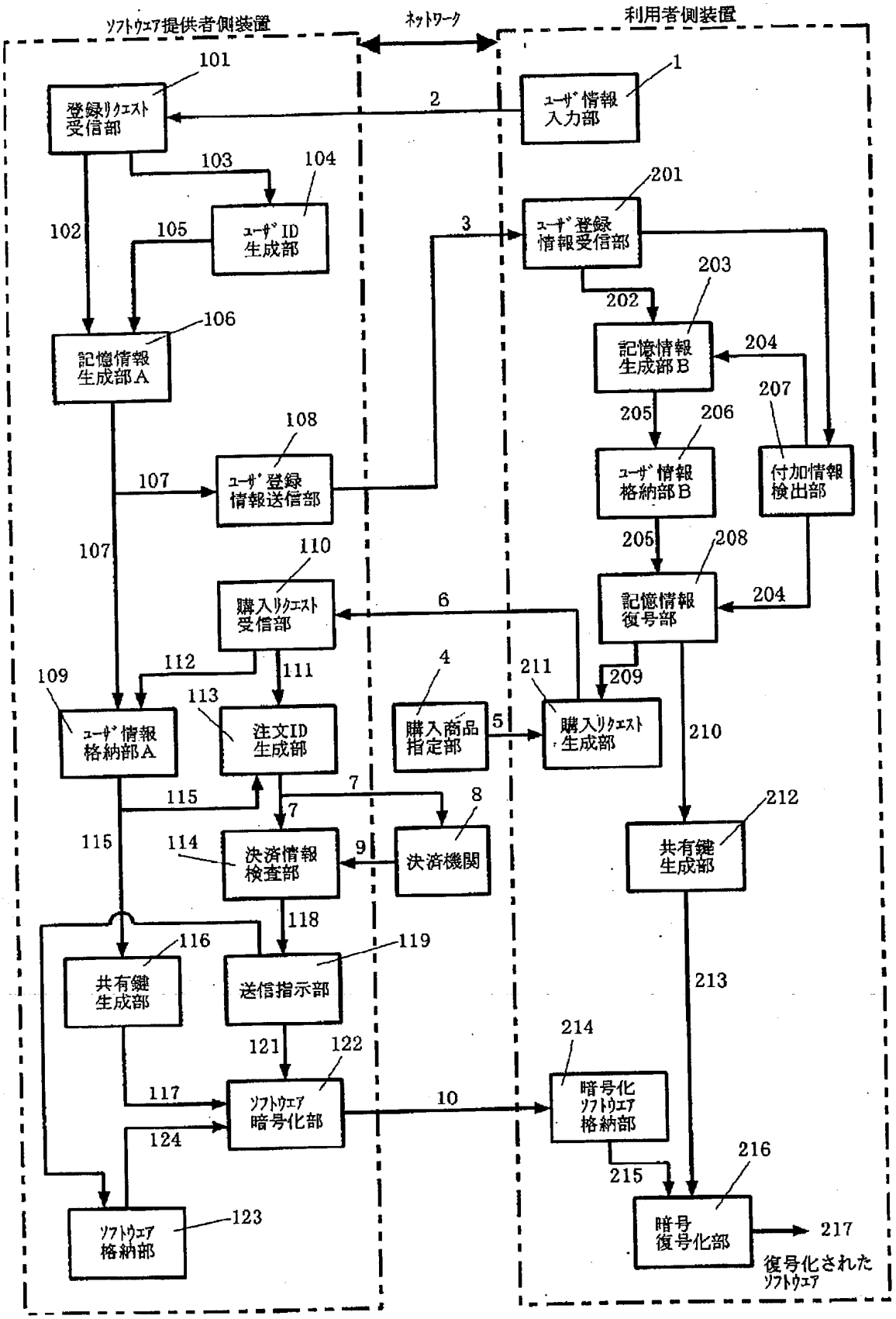
* NOTICES *

Japan Patent Office is not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



[Translation done.]